Healthcare Organization and Hospital Discussion Guide

For Cybersecurity

August 2016

The Oak Ridge Institute for Science and Education (ORISE) is a U.S. Department of Energy (DOE) institute focusing on scientific initiatives to research health risks from occupational hazards, assess environmental cleanup, respond to radiation medical emergencies, support national security and emergency preparedness, and educate the next generation of scientists.

This document was developed by ORISE in collaboration with the Centers for Disease Control and Prevention (CDC) Healthcare Preparedness Activity (HPA) through an interagency agreement with DOE. ORISE is managed by Oak Ridge Associated Universities (ORAU) under DOE contract number DE-AC05-06OR23100.

ACKNOWLEDGMENTS

The Centers for Disease Control and Prevention (CDC) Healthcare Preparedness Activity (HPA) staff would like to thank all of the organizations that helped with the development or review of this tool.

Subject Matter Experts

U.S. Department of Health and Human Services

Centers for Disease Control and Prevention

Office of Public Health Preparedness and Response
Division of State and Local Readiness
Healthcare Preparedness Activity

The following personnel from CDC-HPA contributed to this tool:

Amy Valderrama

Sherline Lee

Dahna Batts

Kelly Dickinson

John Donohue*

Sabrina Harper

Deborah Levy*

Jean Randolph

Office of the Chief Information Officer
Office of the Chief Information Security Officer

Office of the Chief Operating Officer
Office of the Chief Information Officer

*Former HPA staff

Assistant Secretary for Preparedness and Response

Office of the Chief Information Officer
Office of Information Security

Office for Civil Rights

Office of Emergency Management
Critical Infrastructure Protection

Office of the National Coordinator for Health Information Technology
Office of the Chief Privacy Officer

Reviewers

ABS Consulting

Information System Security Manager

Oak Ridge Associated Universities

Information Systems Security Manager

Administrative Support

Oak Ridge Associated Universities

Health, Energy, and Environment Program
Health Preparedness Group

The following personnel from the Oak Ridge Associated Universities (ORAU) Oak Ridge Institute for Science and Education (ORISE) contributed to this tool:

Linda Hodges

Table of Contents

OVERVIEW

Cybersecurity is the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access. Planning for a breach in or attack on an organization's cybersecurity is becoming an increasingly important topic and challenge for healthcare organizations and hospitals that rely heavily on technology for disease prevention and emergency response as well as for support and improvement of patient care. This reliance on technology puts them at increased risk for opportunistic threat actors/adversaries (e.g., hackers) and targeted breaches or attacks.

One of the most problematic elements of cybersecurity is the quickly and constantly evolving nature of security risks. The traditional approach has been to focus resources on the crucial system components and protect against the biggest known threats, which necessitates leaving some less important system components undefended and some less dangerous risks unprotected. Such an approach is insufficient in the current environment. Healthcare organization and hospital computer systems can be attacked by hackers to steal or manipulate patients' financial or medical records or other information, and then be used for criminal activity or to create disorder and generate fear. Cyber attacks threaten healthcare organizations and hospitals' information technology (IT), its underlying security measures, and their employees' ability to care for patients and respond to emergencies. Risks can include the loss of patient information, disruption of care because of software unavailability, loss of confidence in providers because of the perception of inadequate security, power outages, destruction of generators, and risks to the operational integrity of personal medical devices (e.g., implantable cardioverter defibrillators, pacemakers, insulin pumps). In recent years, healthcare organizations and hospitals have increased the use of wireless, personal medical devices and network connections, which places these devices at risk for privacy and security breaches. For example, these wireless devices and network connections can be enabled and modified remotely.

Ensuring cybersecurity requires coordinated efforts throughout an IT system. To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach. The National Institute of Standards and Technology (NIST), for example, recently issued updated guidelines in its risk assessment framework[1] that recommended a shift toward continuous monitoring and real-time assessments.

[1] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

Healthcare organizations and hospitals can prepare for cyber breaches or attacks by implementing measures to secure important systems that have the potential to be threatened. Cybersecurity preparedness involves adequate planning and implementation of a response process, which includes continuous research on and incorporation of lessons learned from

- Actual responses to cyber breaches or attacks and other public health emergencies.
- Facilitated group discussion.
- Simulated exercises and drills.

To assist stakeholders within the healthcare community, the Centers for Disease Control and Prevention (CDC) Office of Public Health Preparedness and Response (OPHPR) developed this *Healthcare Organization and Hospital Discussion Guide for Cybersecurity* (hereafter referred to as *Cybersecurity Discussion Guide*) to support and enhance healthcare organizations and hospitals with addressing cybersecurity. Specifically, this document is intended for personnel whose job responsibilities include cybersecurity preparedness and response planning.

The *Cybersecurity Discussion Guide* focuses on one method (i.e., conducting a discussion-based exercise) to enhance cybersecurity preparedness as part of the threat landscape considered in the creation of an Information System Contingency Plan (ISCP).[2]

> "Information technology (IT) and automated information systems are vital elements in most business processes. Because these IT resources are so essential to an organization's success, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans and procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster."
>
> NIST
> *Contingency Planning Guide for Information Technology Systems*

[2] National Institute of Standards and Technology, *Contingency Planning Guide for Information Technology Systems* http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

Objectives

The objectives of the *Cybersecurity Discussion Guide* are, through group discussion, to

- Identify issues that community healthcare organizations or hospitals would need to address when responding to a cyber breach or attack.
- Develop strategies to address these issues.

Another objective to consider for cybersecurity preparedness is to incorporate these identified strategies, from the aforementioned group discussion, into a community healthcare organization's or hospital's preparedness and response plans. **NOTE:** This objective is outside of the scope of this discussion guide and would be accomplished by those who have oversight and management responsibilities for these plans.

Benefits

The *Cybersecurity Discussion Guide* is intended to help participants identify issues, strengths, and weaknesses associated with response capabilities, communication and information sharing for their healthcare organization or hospital when responding to a cybersecurity incident, and prevention planning. Moreover, the *Cybersecurity Discussion Guide* provides insight into the healthcare organization's or hospital's response to a public health emergency, including communicating and coordinating with other agencies, departments, or organizations. It also provides a catalyst for developing strategies to address the issues and weaknesses identified during the discussion-based exercise.

Situation Categories

Three situation categories are covered in the *Cybersecurity Discussion Guide*:

I. Response Capabilities

II. Communication and Information Sharing

III. Prevention Planning

Format

The *Cybersecurity Discussion Guide* is an activity-based discussion guide (for further information on activity-based discussions, see the section on the Homeland Security Exercise and Evaluation Program methodology on page 5). The *Cybersecurity Discussion Guide* is designed for a small participant group of 8 to 12 people to have a facilitated discussion about a healthcare organization's or hospital's current cybersecurity planning efforts and preparedness and response plans. Prior to starting the activity, a facilitator should be selected to coordinate and lead the discussion using the scenario on page 11 and the situation-based questions provided on page 13.

Discussion questions are divided into three situation categories:

1. Response capabilities.
2. Communication and information sharing.
3. Prevention planning.

The authors of the *Cybersecurity Discussion Guide* recommend that participants review all of the situation-based questions. The facilitator should prioritize the discussion questions according to the group's needs. The authors of the *Cybersecurity Discussion Guide* also recommend that at least two sets of questions from each of the three categories be selected for discussion. With regard to a facilitated discussion-based exercise:

- The facilitator and participants should work through the situations and corresponding sets of questions they select for discussion. Addressing all of the situations and questions or addressing them in any specific order is not a requirement.
- The time required to complete the discussion varies depending on the number of situations and questions the group selects and addresses.
- More than one session can be scheduled to address additional situations and questions.

Prior to a discussion-based exercise, the facilitator decides which of the following two options is more appropriate for introducing the situations and questions to the group. The two options are:

1. **Distribute** the selected situations and corresponding discussion questions to participants 1 to 2 weeks beforehand and instruct them to bring their completed responses to the meeting. This option provides an opportunity for the participants to get a head start on the discussion questions and to delve deeper into known gaps and issues prior to the meeting.
2. **Do not distribute** the selected situations and corresponding discussion questions to participants prior to the meeting; instead, during the discussion-based exercise identify and assess current gaps in planning. This option may require a follow-up meeting to complete all discussion questions. This option also can be used to conduct tabletop exercises.

Recordkeeping

To maximize the benefits of the *Cybersecurity Discussion Guide*, it is recommended that you follow good recordkeeping practices (i.e., document the group discussion). A detailed record of group discussion leads to a more detailed corrective action/improvement plan; therefore, appointing a note-taker or setting up an audio recorder to record the facilitated discussion is important. In particular, any planning or preparation issues that arise from the discussion should be documented. These meeting notes should be used to compile the meeting report discussed in "Next Steps" on page 29.

Homeland Security Exercise and Evaluation Program (HSEEP)

This section provides guidance on utilizing the HSEEP methodology including additional information on exercise design, conduct, and evaluation. The guidance provided is not intended to be inclusive of all relevant information needed to plan an exercise; it is intended for those who are not as familiar with developing exercises.[3]

> "Exercises enable entities to identify strengths and incorporate them within best practices to sustain and enhance existing capabilities. They also provide an objective assessment of gaps and shortfalls within plans, policies, and procedures to address areas for improvement prior to a real-world incident. Exercises help clarify roles and responsibilities among different entities, improve interagency coordination and communications, and identify needed resources and opportunities for improvement.
>
> HSEEP is a capabilities- and performance-based exercise program that provides a set of guiding principles for exercise programs as well as a common methodology for exercise program management, design and development, conduct, evaluation, and improvement planning. HSEEP doctrine is flexible, scalable, and adaptable to the needs of stakeholders across the whole community and is applicable for exercises across all national preparedness mission areas—prevention, protection, mitigation, response, and recovery."[4]

Communities with larger preparedness goals may take an optional step of following HSEEP guidelines to implement the facilitated discussion and then incorporate this discussion into their multi-year training and exercise plans.

Providing Feedback

Feedback or questions about this document can be sent to healthcareprepared@cdc.gov.

---

[3] See FEMA's Protection and Resilience Toolkit, for guiding principles for exercise planning, available at https://emilms.fema.gov/is921/921_toolkit/downloads/nppd_ep.pdf.

[4] The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) *Homeland Security Exercise and Evaluation Program (HSEEP)* https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf.

[This page is intentionally blank]

FACILITATOR GUIDE

According to HSEEP guidance, discussion-based exercises typically work best through facilitated or moderated discussions. Facilitated discussions occur in a plenary session or in breakout groups that are typically organized by discipline or agency/organization. Moderated discussions generally follow breakout group discussions where a representative from each group provides participants with a summary of their facilitated discussion.

Whether the exercise is facilitated or moderated, or both, the facilitator is responsible for keeping discussion relevant to exercise objectives. The facilitator also is responsible for ensuring all objectives and issues are discussed as thoroughly as possible and ensuring relevant discussion questions are asked in order to gather information for desired outcomes.

This *Cybersecurity Discussion Guide* includes the following Facilitator Guide, which is intended to guide facilitators in introducing and helping others with the discussion about cybersecurity in their facilities.

The facilitator should complete several tasks prior to the discussion-based exercise. Suggested tasks are shown in the checklist below.

Pre-Activity Facilitator Checklist

Task	Completed?
1. Review this *Cybersecurity Discussion Guide*.	☐ **Yes**
2. Determine the date, time, and location for the facilitated discussion-based exercise.	☐ **Date** ☐ **Time** ☐ **Location**
3. Identify exercise participants. **NOTE:** When identifying participants, getting management support and including a mix of business, IT, and information security personnel is important in order to obtain views from all relevant stakeholders. Having some participants represent the response team for the remediation of cybersecurity incidents also is important.	☐ **Yes**
4. Send invitations to all exercise participants.	☐ **Yes**

Task	Completed?
5. Appoint a note-taker or set up an audio recorder to record the discussion during the facilitated exercise. In particular, any planning or preparation issues that arise from discussion should be documented. These meeting notes should be used to compile the meeting report discussed in "Next Steps" (on page 29).	☐ **Note-taker** ☐ **Recorder** ☐ **Both**
6. Determine which of the two options for conducting the discussion-based exercise (described under Format on page 4) best fits the group's needs.	☐ **1** ☐ **2**
7. Prioritize the discussion questions (beginning on page 13) according to the group's needs. Selecting at least two sets of questions from each of the three categories for discussion is recommended.	☐ **Yes**
8. Prepare an attendance sheet, including contact information for all participants.	☐ **Yes**
9. Prepare copies of handouts (i.e., agenda, scenario, and list of questions) for all participants. **NOTE:** If using Option 1 (page 4) for the facilitated discussion, remember to provide the questions to participants in advance.	☐ **Yes**
10. Assemble necessary supplies for the activity (e.g., paper, pens, and large index cards).	☐ **Pens** ☐ **Paper** ☐ **Index Cards** ☐ **Other_____**
11. Determine the ground rules for managing the discussion. For example, a. Request participants to avoid crosstalk. b. Request participants to speak in turn only. c. Set time limits for discussion of each question.	☐ **Yes**

Proposed Agenda with Facilitator Notes

Agenda Item	Description
Step 1: Opening (15 minutes)	• Welcome participants and introduce yourself. • Ask participants to introduce themselves to the group. • Explain housekeeping items (e.g., break times, restroom and emergency exit locations, turning off cell phones and pagers). • Give the group your facilitation framework, which includes two basic items: o The **goals** of the session, which includes the objectives. o A **road map** indicating how you will achieve those goals (e.g., your outline or agenda). Comment on any flexibility in timing or content, if applicable. • Define terms, if necessary. **NOTE:** To save time, you may want to have terms defined in a handout or printed on newsprint paper and pasted around the room. • Review your ground rules with the participants. • Appoint a note-taker. • Questions? Ask if anyone has questions before beginning. Answer them, as appropriate.
Step 2: Scenario Presentation (5 minutes)	• Hand out copies of the scenario. • Read or choose a group member to read aloud the scenario, while others follow along. • Questions? Ask if anyone has questions. Answer them, as appropriate.

Agenda Item	Description
Step 3: Facilitated Scenario Discussion (40 to 45 minutes)	• Ask each participant to write their thoughts or ideas about the situation and corresponding questions on a large index card. Ask them to include any questions they have about the topic. • Lead the group through discussion of the scenario and corresponding questions. Encourage participants to answer the questions to the best of their ability, identify issues, and offer solutions (strategies) for the issues.
Step 4: Facilitated Scenario Update Discussion (15 to 45 minutes)	• Present one scenario update and its corresponding questions to the group. • Ask each participant to write their thoughts or ideas about the situation and corresponding questions on a large index card. Ask them to include any questions they have about the topic. • Lead the group through discussion of the situation and corresponding questions. Encourage participants to answer the questions to the best of their ability, identify issues, and offer solutions (strategies) for the issues. • Repeat these steps until all selected situation questions are discussed or until the allotted time elapses.
Step 5: Conclusion (15 minutes)	• Remind the participants about the objectives of the facilitated discussion. • Allow each participant to briefly share their thoughts about the activity (e.g., things they learned). • Schedule follow-up activities/meetings, as necessary. • Thank participants for their attendance and contributions. • Collect index cards and other sources of meeting information.*

***** Following the meeting, the facilitator (or designee) compiles the meeting notes (from the note-taker, the index cards, or the audio recording) as quickly as feasible and distributes them to all participants.

SCENARIO

Instructions

As we begin our facilitated discussion, please read along with the following scenario as it is being narrated to the group. After you have finished reading, please direct any questions to your facilitator.

Background

A new variant of a computer worm[5] has been developed. This worm spreads through networks and removable drives, downloading files and stealing information. The worm is a type of ransomware, which is a program that infects a machine, blocks access to computers by encrypting key components, and demands that a ransom be paid in order for the restriction to be removed. Once the ransomware is activated, it displays a message that the computer has been compromised and will not work until payment is made to the attacker. Until the attacker releases the machine it will not perform any functions, including running services that normally function in the background during machine operations.

In your healthcare organization's or hospital's most recent technology update, IT personnel replaced a large number of older medical devices with newer ones running embedded operating systems. This was done to standardize the IT infrastructure and increase interoperability among computing devices in the healthcare organization's or hospital's network. This update allows easy integration between medical devices that generate reporting, servers that process the reports, and the workstations that are used to query and manipulate the data shared in your healthcare system.

You have received a report from your healthcare organization's or hospital's medical records department that all of the computer screens are locked. Your healthcare organization's or hospital's IT personnel are unable to unlock the computers, and ransomware is suspected.

[5] Webopedia article entitled *The Difference Between a Computer Virus, Worm and Trojan Horse* http://www.webopedia.com/DidYouKnow/Internet/virus.asp.

[This page is intentionally blank]

DISCUSSION QUESTIONS

NOTE: The term *community* in these questions can mean a community, city, or county, depending on your healthcare organization's or hospital's location and setup.

I. Response Capabilities

Question 1

Who would be notified about a cybersecurity incident? For example, would your emergency manager be notified? Would clinical personnel be notified? Who else would be notified?

Question 2

Does a significant cybersecurity situation result in the standing up of your emergency response committee?

- If yes, please describe the plan.
- If no, as a result of this exercise, will you develop a plan for standing up your emergency response committee?

Question 3

In conjunction with your emergency response plan, do you have a continuity of operations plan (COOP) in the event of a cybersecurity incident?

- If yes, please describe the plan.
- If no, as a result of this exercise, do you plan to develop a COOP?

Scenario Update 1

Your IT personnel are having difficulty detecting the worm and controlling its effects.

Question 4

A suggestion may be made to contact outside support.

a. Who would you contact? When and how will you contact them?

b. Do you have agreements with outside groups or relationships in place to seek external assistance?
   - If yes, please describe the groups and agreements and/or the relationships.
   - If no, as a result of this exercise, do you plan to develop agreements? If so, what will the agreements be and with whom?

c. Do you have relationships with other healthcare organizations or hospitals in your region that can assist you?
   - If yes, please describe those relationships.
   - If no, as a result of this exercise, do you plan to develop regional relationships? If so, with whom?

Scenario Update 2

You activate your emergency response plan (cybersecurity response plan, if applicable).

Question 5

a. How do you activate your emergency response (or cybersecurity response) plan?

b. Who is identified as the lead and who will officially activate your healthcare organization's or hospital's plan?

c. What are the criteria that trigger its activation?

d. What security concerns do you have at this time?

e. Do you use an incident management system? If yes, is it web-based? Does it reside on your hospital's server? Would it be accessible in this situation?

f. Does your healthcare organization or hospital have a dedicated command center?
   - If yes, please describe the command center. Is it within your facility?
   - If no, as a result of this exercise, do you plan to dedicate an area for a command center? If so, where will it be located?

Scenario Update 3

Physicians, nurses, and other clinical personnel report that the electronic medical records (EMR) system is not functioning. Patient charting is not possible. You are unable to enter new orders electronically.

Question 6

a. How does not being able to enter new orders electronically affect how care is delivered in your healthcare organization or hospital?

b. What contingency plans (e.g., paper charting) do you have in place for this type of event?

c. How do you communicate with physicians, nurses, and other personnel to make them aware of the situation? Are these communication methods or channels dependent on the use of technology?

d. What actions will you take to ensure lines of communication remain open?

e. What actions will you take to maintain patient safety, including medication safety?

f. What other kinds of decisions have to be made?

Scenario Update 4

Upon further investigation, you discover that

- Dr. Smith is an attending physician at your healthcare organization or hospital and has children at home who frequently download music and games from the Internet onto their home computer. During one of these instances, they unknowingly downloaded a computer worm onto their home computer and infected the computer.

- Dr. Smith was scheduled to present at the hospital's Grand Rounds. He had been working on his presentation on his office computer, but had some additional edits to make later in the day at home. He saved his presentation onto a Universal Serial Bus (USB) flash drive that he received at a recent medical conference. Once home, he plugged the USB drive into his home computer, finished his presentation, and saved the updated version onto the USB drive, which became infected with the computer worm from his computer.

- Upon arriving at the hospital on the day of his presentation, he used the infected USB device to transfer the files he was working on to a workstation at the hospital. The device infected the hospital workstation with the ransomware worm. While the worm began encrypting the user files on the workstation, it also began to search the healthcare organization's or hospital's local network looking for vulnerabilities such as "open file shares" to allow it to infect other machines.
- For the next 30 days, nothing abnormal was seen by users; however, the worm was spreading throughout the hospital network.

Question 7

a. Does this information impact your response? How so?

b. What additional actions do you take?

c. Do current IT policies prevent this type of scenario from occurring?

- If yes, describe the IT policy (or policies).
- If no, as a result of this exercise, do you plan to develop an IT policy (or policies) to prevent this type of scenario from occurring?

Scenario Update 5

The computer worm begins exfiltrating (i.e., the unauthorized transfer of data from a computer) patient billing information off-site, including patient identifiers and insurance information. The healthcare organization's or hospital's insurance and payment systems are not operational.

Question 8

a. Who do you need to inform about this situation?

b. Was the legal department notified and involved in the breach response?

c. What external organizations are notified of the breach?

d. If you use outside vendors, do they provide a contingency plan?

e. What do your service-level agreements (SLAs)[6] cover in the event of a cybersecurity incident?

f. How do you coordinate and inform patients of this breach, including current and former patients?

g. How does this breach impact your ability to see or admit new patients?

h. Do you have a plan in place on how to implement the Health Insurance Portability and Accountability Act (HIPAA) Security Rule[7] notification to individuals?

i. Does your business continuity plan provide alternative processes that could be used to sustain operations in this scenario?

- If yes, describe this process.
- If no, as a result of this exercise, do you plan to develop any alternative processes, and add it to your business continuity plan, which could be used to sustain operations in this type of scenario?

Scenario Update 6

You receive an urgent notification that the ventilation systems have been affected by the cyber attack. As a result, negative air pressure rooms are not functioning properly. You have three negative pressure rooms; two of them are occupied with patients who have active tuberculosis; one is suspected to have multidrug-resistant tuberculosis.

Question 9

a. Do you have backup power for your ventilation systems?

b. If you do not have a back-up system, what happens?

[6] An SLA is a document describing the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved.

[7] HIPPA Security Rule Crosswalk to NIST Cybersecurity Framework http://www.hhs.gov/sites/default/files/NIST%20CSF%20to%20HIPAA%20Security%20Rule%20Crosswalk%2002-22-2016%20Final.pdf.

c. Who will you notify concerning the interruption and why?

d. How will you notify them?

e. How do you maintain the safety of your patients and personnel? What actions will you take to protect other patients and personnel?

f. Do you have existing relationships or agreements with other healthcare organizations or hospitals that are in close proximity (within your region) that can assist with or address this type of scenario?

Scenario Update 7

The heating, ventilation, and air conditioning (HVAC) system has been affected and is disabled. This causes health and safety risks to patients who could be adversely affected by lack of climate control in the building. Pharmaceuticals may be adversely affected by the lack of cooling.

Question 10

a. How do you maintain the health and safety of your patients and personnel?

b. Do you have existing plans to address this type of situation?

- If yes, describe those plans.
- If no, as a result of this exercise, will you develop plans to address this type of situation?

c. How do you ensure that medications are kept at appropriate temperatures given the lack of air conditioning?

Scenario Update 8

Other systems in your healthcare organization or hospital have the potential to be negatively affected by this cybersecurity incident.

Question 11

a. How will you maintain the health and safety of your patients and personnel in each of the following areas?

- Emergency department
- Intensive Care Unit
- Critical/Cardiac Care Unit
- Surgical areas (outpatient and inpatient)
- Laboratory
- Pharmacy

b. What actions will you take to maintain continuity of operations?

Scenario Update 9

Similar cyberattacks are being reported in other parts of your region and state. Multiple healthcare organizations, hospitals, and clinics are affected. The governor has declared a statewide emergency.

Question 12

a. What are some of your key concerns, if other healthcare organizations' or hospitals' systems are impacted?

b. What critical information will you require to help leaders in your local area, region, or state make decisions?

c. Do you have the ability to coordinate with other healthcare organizations or hospitals in your local area, region, or state?

d. How will you be notified of cybersecurity incidents in other healthcare organizations or hospitals? How will you be notified that a state of emergency has been declared?

e. Do you have procedures in place that will be instituted in the event that a state of emergency is declared?

   - If yes, describe those procedures.
   - If no, as a result of this exercise, will you develop procedures to address the declaration of a state of emergency?

f. In the face of a cybersecurity incident, does your emergency response plan prescribe to an incident management structure? If yes, describe this structure, including chain of command, the personnel who would make up its key components, and their roles and responsibilities.

g. Do you have a regional cybersecurity plan?

   - If yes, describe the plan.
   - If no, as a result of this exercise, will you develop a regional cybersecurity plan?

h. How does your incident management structure interact with external emergency operations centers (EOCs) and incident command systems (ICSs)?

i. What information is shared between your healthcare organization or hospital and these EOCs/ICSs?

Scenario Update 10

A nationally renowned cancer researcher is employed by your healthcare organization or hospital system and is conducting a large randomized, controlled trial. He houses his clinical trial data on your facility's server. He notifies you that his data are encrypted and he is unable to access the data. Later that day, he notifies you that he has received a demand for monetary payment to release the data. You suspect that ransomware has encrypted his data.

Question 13

a. What are your key concerns?

b. What approach will you take to manage this situation?

c. When do you need to notify the grant funders (e.g., National Institutes of Health) about the situation?

d. How do you manage the potential loss of protected health information of study participants?

Scenario Update 11

You are notified of a nearby bus crash, involving 25 retired persons on a tour bus. Several of your key systems, including your intake and EMR systems, are impacted by the worm. You are concerned about your ability to care for these patients.

Question 14

a. What are some of your key concerns?

b. Will you accept these patients or do you divert them to another facility? What if other facilities also are infected with the worm?

c. Do you have the ability to coordinate patient care with other healthcare organizations or hospitals in your region? If no other facility is available, how do you care for these patients given your current situation?

Scenario Update 12

Your healthcare organization's or hospital's IT department has been able to isolate and remove the ransomware affecting the facility. Your services have been restored and your systems are operating normally. You determine that deactivation of your response is appropriate.

Question 15

a. Who is responsible for deactivation?

b. What are the criteria that trigger deactivation?

c. What procedures are in place to guide the resumption of normal operations?

d. Do you have an incident response plan that includes documenting lessons learned and next steps?

- If yes, describe the plan.
- If no, as a result of this exercise, will you develop an incident response plan?

II. Communication and Information Sharing

Scenario Update 13

Upon recognition of the cybersecurity incident, you determine communication priorities and activities.

Question 1

a. Do you have an existing plan in place that addresses communication in the event of a cybersecurity incident?

b. Does your communication plan define roles and responsibilities, key points of contact (e.g., calling tree), and have detailed procedures for this cybersecurity incident?

- If yes to a. and b., describe the communication plan.
- If no to a. and b., as a result of this exercise, will you develop a communication plan?

c. How is this cybersecurity incident communicated to personnel throughout your healthcare organization or hospital?

d. To whom or to what department(s) is the alert initially communicated?

e. Who communicates this alert to your local public health or emergency management agency?

f. To whom do you communicate with at your local public health or emergency management agency? How do you communicate your situation?

g. What other communication should occur and with whom?

h. How will you control the news media at your healthcare organization or hospital?

i. How will you deal with the families who want to get their family members out of your hospital?

Scenario Update 14

Your healthcare organization or hospital is beginning to receive an increased number of calls and requests for information from patients and their family members. They want to know if their personally identifiable information/protected health information is secure and what your facility's personnel are doing about the situation.

Question 2

a. What public relations issues do you foresee with this scenario?

b. Do you have a plan in place to address these issues?

- If yes, describe your communication plan.
- If no, as a result of this exercise, will you develop a communication plan to address these public relations issues?

c. What actions will you take to provide patients and their family members with the information they seek and thus, reduce call volume? How will you communicate information to personnel and the public?

d. What information will your messaging include?

Scenario Update 15

Hospital personnel report that the telephone systems (internal and external) are affected and they are unable to make or receive phone calls. Your healthcare organization's or hospital's paging system is not operational, including the notification system for emergencies (e.g., code blue).

Question 3

a. What issues does this situation pose to your operations?

b. What issues does this situation pose to your response?

c. How would your healthcare organization or hospital respond to this situation?

d. How will you communicate information and instructions to personnel?

e. How will you communicate information to patients and visitors?

Scenario Update 16

Your payroll systems have been affected. You may not be able to pay your employees on the upcoming pay date. When employees hear about this, the human resources (HR) department receives numerous complaints from employees.

Question 4

a. Does your HR department have a plan in place to address this situation?

- If yes, describe the plan.
- If no, as a result of this exercise, will you develop a plan?

b. Do you have back-up systems or additional support for payroll?

- If yes, describe the back-up system and or the additional support you will use.
- If no, as a result of this exercise, will you develop a back-up system or make plans for additional support assistance?

c. What actions will you take to communicate this issue and decisions to personnel?

III. Prevention Planning

Question 1

a. How might you prevent a scenario like the one presented?

b. Do you have policies and procedures in place that restrict/guide/monitor the use of

- External flash drives?
- Sharing files from home or office?
- Downloading files from the Internet?
- Installation of software by personnel?
  - If yes, would your policies/procedures have prevented the introduction of the worm into your network?
  - If no, what policies and procedures would be beneficial to prevent this situation from occurring in your healthcare organization or hospital?

c. Do you have an established cybersecurity program? What does it include? Are your personnel aware of the program? Do they have access to the program guidelines?

NOTE: Question 1c. is a suggested example of a high-level question to identify the existence or lack of a cybersecurity program or framework/structure within the organization.

Question 2

a. Do you have cybersecurity defined in your emergency plan?

- If yes, does it cover a situation such as this? How?
- If no, as a result of this exercise, do you plan to add it to the plan?

b. Does your business continuity plan also address cybersecurity scenarios?

c. Do you have an Information System Contingency Plan (see page 2)?

Question 3

a. Do your personnel know how to identify cybersecurity incidents?

- If yes, how?
- If no, as a result of this exercise, do you plan to conduct personnel training?

b. Do they know who to call when a cybersecurity incident occurs?

- If yes, who? Is there a calling tree list?
- If no, as a result of this exercise, do you plan to develop a calling tree list and conduct personnel training?

c. Are personnel required to attend security awareness training?

- If yes, does the training include information on how to identify cybersecurity incidents? How often is refresher training provided?
- If no, as a result of this exercise, do you plan to develop training or add information about cyber incidents to the current training?

NEXT STEPS

As pointed out in the Overview section, the objectives of this *Cybersecurity Discussion Guide* are, through group discussion, to

- Identify issues that community healthcare organizations or hospitals would need to address when responding to a cyber breach or attack.
- Develop strategies to address these issues.

Another objective to consider for cybersecurity preparedness also was pointed out, which is to incorporate these strategies identified from the aforementioned group discussion into a community healthcare organization's or hospital's preparedness and response plans. However, this objective would be accomplished outside the scope of this *Cybersecurity Discussion Guide*.

After you have completed a facilitated discussion about your healthcare organization's or hospital's current cybersecurity planning efforts and preparedness and response plans, the next step is to issue a written report of the group discussion. This report should include

a. A compilation of the group discussion.

b. Identification of

   - Issues in response capabilities and resource availability.
   - Strategies for addressing these issues.
   - The person(s) responsible for maintaining the cybersecurity preparedness and response plans.
   - Next steps for implementing the identified strategies.
   - The person(s) responsible for implementing the next steps.

Once this report is issued, those responsible for maintaining the cybersecurity preparedness and response plans can make the suggested corrective actions and improvements.

[This page is intentionally blank]

CONCLUSION

The use of the *Cybersecurity Discussion Guide* can stimulate thought and promote discussion on cybersecurity preparedness and response. Several key issues should have been identified as well as strategies for addressing them. These strategies should be documented in a written report and incorporated into your healthcare organization's or hospital's cybersecurity preparedness and response plan.

Cybersecurity planning is an ongoing process. Discussion should continue, whether within the framework of this *Cybersecurity Discussion Guide* or in a more formal setting. The overarching planning goal is continued improvement, with planning adjustments being made as needed.

Additionally, this discussion-based exercise will present some unique communication challenges. Once a cyber breach becomes public knowledge, communicating and visually managing the situation is critical; therefore, communication planning and training should be a consideration.

[This page is intentionally blank]